Australian Government
Department of Home Affairs

Department of Home Affairs Submission on the capability of law enforcement to respond to cybercrime

Joint Committee on Law Enforcement

15 December 2023

Introduction

The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement's inquiry on the capability of law enforcement to respond to cybercrime. The Department and the National Cyber Security Coordinator (the Coordinator)—supported by the National Office of Cyber Security (NOCS)—have a number of responsibilities in relation to cybercrime awareness and response, as well as cyber security policy generally.

The Department is responsible for supporting the Minister for Home Affairs and the Minister for Cyber Security in the development of cyber security policy, including the implementation of the *2023–2030 Australian Cyber Security Strategy* (the Strategy, **Attachment A** refers). The Department and the Coordinator also engage with international partners to share information and gain global perspectives in an effort to strengthen global cyber security.

On 1 May 2023, the National Office of Cyber Security (NOCS) was established within the Department, to support the role of the Coordinator. The Coordinator and the NOCS provide a single point of coordination across government to deliver cyber security responsibilities, and lead the coordination of whole of government action (including cross-jurisdictional) to support Australia's response to major cyber incidents. The Coordinator is responsible for providing strategic direction and oversight of cyber security policy development across government, including the implementation of policy, program and legislative measures in the Strategy.

Current policy and coordination efforts

2023-2030 Australian Cyber Security Strategy

The recently released Strategy highlights the importance of cyber security to all Australians. The Strategy sets out Government's vision to become a world leader in cyber security by 2030 and how it will do so by harnessing individuals and businesses to tackle cyber problems through stronger public-private partnerships. The Strategy takes a whole of nation approach to building cyber resilience through six national cyber shields.

Under Shield One, the Government will ensure citizens and businesses are better protected from cyber threats, and can recover quickly following a cyber attack. The Government will do so by further enhancing efforts to deter and disrupt cybercrime by: building on efforts already underway through the Australian Federal Police and Australian Signals Directorate; co-designing options with industry to mandate ransomware reporting to enhance our national threat picture; increasing awareness raising efforts to ensure Australians can better safeguard themselves again cybercrime; and providing enhanced support to individuals and businesses following a cyber incident. These actions will ensure responsibility for cyber deterrence sits with those most capable of taking defensive action. The Government will use all lawful and appropriate levers to deter and disrupt cyber criminals.

Government-led cyber security exercises

The Cyber Security Response Coordination Unit (CSRCU), within the NOCS, regularly conducts cyber security exercises with industry across a range of sectors, discussing different powers and frameworks that may be triggered in response to a nationally significant cyber security event. The attendance of law enforcement agencies (LEAs) at these events has positively impacted industry's understanding of the role of LEAs in cyber security incident response, and the benefits of early notification of incidents which allows LEAs to more effectively contain harms. These exercises hence build the relationship between LEAs and industry, as well as increase industry's understanding of how to use LEAs in the case of a cyber incident.

Australian Government Crisis Management Framework

The Australian Government Crisis Management Framework (AGCMF) and its component bodies are designed to respond to incidents that might reach the threshold for a crisis, but may not directly coordinate all elements of consequence management that may be required to respond to a cyber security incident.

Within the AGCMF, the Australian Cyber Response Plan (AUSCYBERPLAN) will be the coordination arrangement for the Australian Government's response to cyber incidents. It will provide an overview of the Australian Government's various cyber incident response coordination arrangements, describes response activities covered by those arrangements, and identifies the departments and agencies responsible for those arrangements.

The AUSCYBERPLAN will recognise the separation between the consequence management functions of the CSRCU, and the operational activities of Commonwealth, State and Territory LEAs. The CSRCU can support policing activities if requests for support are made, including through enabling joint briefings with the impacted entity, however LEAs are responsible for managing the collection of information in relation to a cyber incident insofar as it relates to their role in investigating a crime. During cyber security incidents, the NOCS also works closely with LEAs through the National Cyber Security Committee, which is the mechanism for inter-jurisdictional coordination for technical responses to national cyber security incidents.

International collaboration

Since 2021, Australia has been a leading member of the international Counter Ransomware Initiative (CRI), a White House-led initiative that is designed to build collective global resilience to ransomware and seeks to defend and disrupt the ransomware threat. CRI members discuss and share information relating to tactics, techniques and procedures which can be used in turn to inform members' respective domestic ransomware policies. At the third international CRI Summit in Washington D.C. on 31 October – 1 November 2023, Australia joined 48 CRI members, including the United States, to a non-binding statement of intent that relevant institutions under national government authorities should not give into ransomware extortion demands. Since January 2023, Australia (through the Department) chairs the CRI's International Counter Ransomware Taskforce (ICRTF), which comprises 27 CRI members including INTERPOL. The ICRTF builds cross-sectoral capabilities to reduce and prevent ransomware attacks, creates and shares resources to develop national capabilities, and supports transnational operations, including cyber security operations and responses in our nearest region.